

DATENSCHUTZ - D01

Stand: Februar 2018

Ihr Ansprechpartner
Ass. iur. Kim Pleines
E-Mail
kim.pleines@saarland.ihk.de
Tel.
(0681) 9520-640
Fax
(0681) 9520-690

EU-Datenschutz-Grundverordnung

I. Hintergrund

Am 24.05.2016 ist nach mehr als vierjährigen Verhandlungen die EU-Datenschutz-Grundverordnung (DSGVO) in Kraft getreten. Mit der Verordnung hat die europäische Union das Datenschutzrecht innerhalb Europas auf eine neue Ebene gestellt. Die DSGVO löst die bisherige Datenschutzrichtlinie aus dem Jahr 1995 ab und regelt den Datenschutz innerhalb der EU weitgehend **einheitlich und verbindlich**. Grund für die Unterbreitung des ersten Entwurfs der Kommission für ein harmonisiertes europäisches Datenschutzrecht waren sowohl die **uneinheitliche Umsetzung** als auch eine **unterschiedliche mitgliedstaatliche Auslegungspraxis** der Richtlinie. Nach einer Umsetzungsfrist von zwei Jahren **gilt die Verordnung ab dem 25.05.2018 unmittelbar in allen Mitgliedstaaten der EU**. Sie muss nicht mehr wie die alte Datenschutzrichtlinie durch nationale Gesetze umgesetzt werden. Insgesamt besteht die DSGVO aus 99 Artikeln und annähernd doppelt so vielen Erwägungsgründen, die der Erläuterung dienen sollen.

Ziel der Verordnung ist es, europaweit ein **einheitliches Datenschutzniveau** zu erreichen sowie den Datenschutz an die zwischenzeitliche **technische Weiterentwicklung des Internets** und die **fortschreitende wirtschaftliche Globalisierung** anzupassen.

Obwohl die Staaten von den meisten Regeln aufgrund der Vereinheitlichung nicht mehr abweichen können, lässt die Verordnung für bestimmte Bereiche wie den Beschäftigtendatenschutz oder den betrieblichen Datenschutzbeauftragten - im Rahmen von **Öffnungsklauseln** - den einzelnen Mitgliedstaaten die Möglichkeit nationaler Regelungen.

In Deutschland wird dementsprechend ab dem 25.05.2018 zusätzlich zur DSGVO das neue DSAnpUG-EU (Datenschutz-Anpassungs- und Umsetzungsgesetz EU) das bis dahin geltende BDSG (Bundesdatenschutzgesetz) ablösen.

Beim Datenschutz geht es um den **Schutz personenbezogener Daten**. Davon sind alle Informationen umfasst, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen, wie Name, Geburtsdatum oder IP-Adresse. Der Anwendungsbereich der DSGVO ist sehr weit gefasst. Es geht um den Schutz dieser Daten als Ausfluss des **Persönlichkeitsrechts** einer jeden Person.

Wichtig: Es gibt mit Inkrafttreten der Verordnung keine Schonfrist. Unternehmen sollten die Zeit bis zum **25.05.2018** nutzen, um ihre Geschäftsprozesse datenschutzkonform zu gestalten.

II. Was sind die Grundsätze der DSGVO?

Der Datenschutz wird durch die DSGVO nicht neu erfunden. Es bleibt grundsätzlich bei den bisherigen Zielen und Grundsätzen des Datenschutzes. Diese Grundsätze, die bei einer automatisierten Verarbeitung personenbezogener Daten zu beachten sind, werden in [Art. 5 und Art. 6 der DSGVO](#) aufgelistet:

1. Verbot mit Erlaubnisvorbehalt:

Grundsätzlich ist eine Datenverarbeitung verboten, da die Verarbeitung in das verfassungsrechtlich geschützte Persönlichkeitsrecht einer jeden Person eingreift. Eine Datenverarbeitung kann jedoch dann vorgenommen werden, wenn sie beispielsweise gesetzlich erlaubt ist oder auf einer Einwilligung der betroffenen Person beruht.

2. Rechtmäßigkeit:

Die Verarbeitung von Daten ist dann rechtmäßig, wenn sie auf einer entsprechenden Grundlage beruht (Rechtsgrundlage, Einwilligung usw.) und der Zwecke der Verarbeitung von der Rechtsgrundlage bzw. der Einwilligung umfasst ist.

3. Transparenz:

Die betroffene Person muss wissen, wer welche Daten für welchen Zweck verarbeitet. Daher gibt es umfangreiche Betroffenenrechte (z. B. Informationspflichten, Auskunftsrechte, Recht auf Berichtigung der Daten, Widerspruchsrecht).

4. Zweckbindung:

Die DSGVO sieht eine enge Zweckbindung vor. Personenbezogene Daten dürfen nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden. Ausnahmen sind vorgesehen für sog. kompatible Zwecke, also Zweckänderungen, die aber mit dem ursprünglichen Zweck eng zusammenhängen.

5. Datenminimierung:

Es dürfen nur die personenbezogenen Daten verarbeitet werden, die für die Zweckerreichung notwendig sind.

6. Richtigkeit:

Die Daten müssen richtig sein, weshalb alle angemessenen Maßnahmen zu treffen sind, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

7. Speicherbegrenzung:

Personenbezogene Daten dürfen nur so lange gespeichert werden, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist (Datensparsamkeit). Sind sie nicht mehr erforderlich, müssen sie gelöscht werden. Zudem sind alle Möglichkeiten zur Anonymisierung von Daten zu nutzen.

8. Integrität und Vertraulichkeit:

Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der Daten gewährleistet. Die DSGVO verknüpft sehr stark den Datenschutz mit der Technik. Die IT-Verfahren müssen somit schon von Anfang an darauf ausgerichtet sein, möglichst wenig personenbezogene Daten verarbeiten zu können (privacy by design).

9. Rechenschaftspflicht:

Dies ist der wichtigste Aspekt aller Grundsätze. Die Einhaltung der dargestellten Grundsätze für die Verarbeitung personenbezogener Daten ist durch den Verantwortlichen nachzuweisen. Dazu ist ein Datenschutzmanagement notwendig - natürlich abhängig von der Größe des Unternehmens, der personenbezogenen Daten, die verarbeitet werden und der Menge und der Qualität der Daten. Auch in kleineren und mittleren Unternehmen muss ein Mindestmaß an Dokumentation vorhanden sein, um die Einhaltung des Datenschutzes nachweisen zu können.

III. Wann dürfen Daten verarbeitet werden?

Prinzipiell gilt bei der Datenverarbeitung der Grundsatz, **dass jegliche Verarbeitung personenbezogener Daten verboten ist, es sei denn, es gibt eine Erlaubnis dafür**. Obwohl dieser Grundsatz mit Blick auf die fortschreitende Digitalisierung manch einem befremdlich erscheinen mag, ist er die Konsequenz des **Grundrechts auf informationelle Selbstbestimmung** und Bestandteil der Europäischen Menschenrechtskonvention.

In [Art. 6 der DSGVO](#) werden die verschiedenen **Zulässigkeitsgründe** für eine Verarbeitung angeführt:

1. Einwilligung:

Die Datenverarbeitung ist rechtmäßig, wenn die betroffene Person ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben hat (mehr dazu unter Punkt 4).

2. Vertrag:

Daten, die zur Erfüllung eines Vertrags oder einer vorvertraglichen Maßnahme benötigt werden, dürfen zulässig erhoben werden.

3. Rechtliche Verpflichtung:

Sofern ein anderes Gesetz die Erhebung und Verarbeitung von personenbezogenen Daten vorsieht, liegt eine rechtliche Verpflichtung für den Verantwortlichen vor. Eine Verarbeitung der Daten zur Erfüllung dieser Pflicht ist dann in dem gesetzlich vorgegebenen Rahmen zulässig.

4. Wahrung berechtigter Interessen:

Die Verarbeitung ist rechtmäßig, wenn sie für die Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist, und die Interessen der betroffenen Person diese Interessen nicht überwiegen.

5. Weiterverarbeitung:

Unter bestimmten Voraussetzungen können personenbezogene Daten auch weiterverarbeitet werden, wenn die Verarbeitung nicht mehr dem ursprünglichen Zweck entspricht. Hierfür muss der neue Zweck mit dem alten kompatibel, darf also für die betroffene Person nicht überraschend sein. Hierfür muss aber der Verantwortliche eine genaue - dokumentierte - **Prüfung anhand der in Art. 6 Abs. 4 festgelegten Kriterien** durchführen, ob der neue Zweck mit dem ursprünglichen Zweck übereinstimmt. Ergibt die vom Verantwortlichen durchgeführte Prüfung, dass der Zweck nicht kompatibel ist, ist eine darauf gestützte Verarbeitung unzulässig, es sei denn, es wird für den neuen Zweck wiederum eine Einwilligung eingeholt.

Die Prüfung umfasst insbesondere folgende Punkte:

- jede **Verbindung zwischen den Zwecken**
- der **Zusammenhang der Erhebung der Daten**, insbesondere hinsichtlich des Verhältnisses zwischen der betroffenen Person und dem Verantwortlichen
- die **Art der personenbezogenen Daten** (z. B. besonders sensible Daten)
- die **möglichen Folgen** der beabsichtigten Weiterverarbeitung für die betroffenen Personen
- Vorhandensein geeigneter Garantien wie **Verschlüsselungen oder Pseudonymisierungen** der Daten.

IV. Was ist bei Einwilligungen zu beachten?

Nach [Art. 4 Nr. 11 DSGVO](#) bezeichnet der Ausdruck „Einwilligung der betroffenen Person“ jede **freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung** in Form einer Erklärung oder einer sonstigen **eindeutigen bestätigenden Handlung**, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten **einverstanden** ist.

Bedingungen für die Einwilligung werden in [Art. 7 der DSGVO](#) geregelt. Die Einwilligungserklärung muss in **verständlicher, leicht zugänglicher Form, in klarer und einfacher Sprache** sein. Sie darf nicht in den AGB oder in der Datenschutzerklärung „**versteckt**“ werden, sondern ist getrennt von anderen Inhalten darzustellen.

1. Freiwilligkeit:

Die Verarbeitung von personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ist zulässig, wenn die betroffene Person hierin **ausdrücklich eingewilligt** hat. Es gilt auch weiterhin das bekannte Prinzip, dass eine Einwilligung freiwillig und **ohne jeden Zwang** abgegeben werden muss. In [Erwägungsgründen 43](#) der DSGVO wird eingehend erläutert, dass eine Einwilligung dann nicht als freiwillig abgegeben gilt, wenn zwischen den Parteien ein **klares Ungleichgewicht** besteht und es deshalb unwahrscheinlich ist, dass die Einwilligung ohne Zwang abgegeben worden ist.

2. Informiertheit:

An dieser Stelle greift die DSGVO auf anerkannte Grundsätze zurück. **Blankoeinwilligungen** genügen danach nicht den festgelegten Ansprüchen. Vielmehr muss die betroffene Person unzweifelhaft **nachvollziehen** können, **welche personenbezogenen Daten zu welchem Zweck und von wem verarbeitet werden**. Die **verantwortliche Stelle** muss in diesem Zusammenhang ausdrücklich genannt werden. Dient eine Verarbeitung mehreren Zwecken, müssen alle **Zwecke** ausdrücklich genannt und die Einwilligung für sämtliche Zwecke eingeholt werden.

3. Eindeutigkeit:

Des Weiteren muss das Einverständnis in die Datenverarbeitung eindeutig zum Ausdruck kommen. **Stillschweigen, bereits angekreuzte Kästchen** („Ich willige in die Verarbeitung meiner Daten ein“) oder **Untätigkeit** der betroffenen Person stellen daher keine Einwilligung dar. Die alte Opt-Out Wahlmöglichkeit ist somit unzulässig.

4. Kopplungsverbot:

Im Zusammenhang mit der Freiwilligkeit der Einwilligung steht das in der Datenschutz-Grundverordnung nunmehr erstmals ausdrücklich geregelte, generell geltende sog. Kopplungsverbot. Danach dürfen Verantwortliche Verträge oder die Erbringung von Dienstleistungen nicht davon abhängig machen, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten, die für die Erfüllung des Vertrages nicht erforderlich sind, einwilligt. Umstritten ist, ob das Kopplungsverbot auch dort Anwendung findet, wo Nutzern entgeltfreie - weil zum Beispiel werbefinanzierte - Inhalte und Dienstleistungen angeboten werden. Die Klärung dieser Streitfrage bleibt abzuwarten. Bis zur rechtsverbindlichen Entscheidung der Frage ist es jedoch ratsam, sich an dem Wortlaut des [Art. 7 Abs. 4 der DSGVO](#) zu orientieren.

5. Form:

Die DSGVO sieht keine bestimmte Form für die Erteilung einer Einwilligung vor. Sie kann **schriftlich, elektronisch oder mündlich** erfolgen. Wichtig ist, dass eine **unmissverständlich** abgegebene Willensbekundung in **Form einer Erklärung** oder einer sonstigen **eindeutig bestätigenden Handlung**, mit der die betroffene Person ihr sein Einverständnis zur Datenverarbeitung signalisiert, erkennbar ist. Die Frage, welche Form sich als praktikabel erweist, muss zukünftig geklärt werden. Aufgrund der Tatsache, dass Datenverarbeiter zwingend der **Nachweispflicht** aus Artikel 5 Absatz 2 DSGVO unterliegen, werden Einwilligungen in der Praxis wohl weiterhin in **Schriftform** eingeholt werden. Nur so kann die Eindeutigkeit der Einwilligung dokumentiert werden.

***Wichtig:** Die Möglichkeit der **formlosen Erklärung** einer Einwilligung wurde neu eingeführt. Es muss allerdings beachtet werden, dass die **Nachweispflicht** auch für formlos erklärte Einwilligungen gilt!*

Widerrufsmöglichkeit:

Die betroffene Person muss ausdrücklich auf ihr Recht hingewiesen werden, dass **sie ihre Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann**. Dieser Hinweis ist ebenso wie die Einwilligungserklärung selbst in **einfacher, verständlicher Sprache** zu verfassen und **leicht zugänglich** zu machen. Der Hinweis auf das Widerrufsrecht muss **vor Abgabe der Einwilligung** erteilt werden.

Fortgeltung bisheriger Einwilligungen:

Von besonders großer Bedeutung für Unternehmen ist die Frage, ob die bislang nach BDSG und TMG eingeholten Einwilligungen fortgelten. Nach [Erwägungsgrund 171](#) der DSGVO gelten bisher erteilte Einwilligungen danach fort, sofern sie **rechtmäßig eingeholt** wurden. Erforderlich ist dafür, dass:

- der **Grundsatz der Freiwilligkeit** beachtet wurde,
- das **Koppelungsverbot** berücksichtigt wurde und
- der **Hinweis auf den jederzeitigen Widerruf** erfolgte.

Wichtig: *Verstoßen alte Einwilligungen allerdings gegen die aufgezählten Punkte, gelten sie nicht fort und müssen erneut eingeholt werden. Es ist für alle **Betroffenen** ratsam, bestehende Einwilligungen speziell daraufhin zu prüfen und den **Einwilligungsprozess** bei Handlungsbedarf kurzfristig **anzupassen**.*

*Erweisen sich Einwilligungen grundsätzlich nach den oben genannten Kriterien als **unwirksam**, ist das Vorliegen der Einwilligung nicht durch den Verantwortlichen nachweisbar und liegen auch keine sonstigen gesetzlichen Erlaubnistatbestände vor, ist die Verarbeitung der personenbezogenen Daten **unzulässig** und kann mit einem **Bußgeld** belegt werden.*

V. Was ist neu?

1. Die wichtigsten Neuerungen der DSGVO für Unternehmen sind:

- **Wegfall des Schriftformerfordernisses** bei Einwilligungen:
Die DSGVO sieht keine bestimmte Form für die Erteilung einer Einwilligung vor. Sie kann **schriftlich, elektronisch oder mündlich** erfolgen (mehr dazu unter Punkt IV).
- **Erweiterung der Informationspflichten:**
In [Art. 13 und Art. 14 DSGVO](#) wurden die Informationspflichten gegenüber den Betroffenen erheblich **erweitert**, um für eine bessere **Nachvollziehbarkeit der Datenverwendung** zu sorgen. Der Betroffene ist vor Erhebung von personenbezogenen Daten in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache über die Verwendungsgesichtspunkte zu informieren.

Im Einzelnen sind dies:

- Name und Kontaktdaten des für die Datenerhebung Verantwortlichen
- die Kontaktdaten des Datenschutzbeauftragten
- die Zwecke und die Rechtsgrundlage der Verarbeitung
- das berechtigte Interesse des Verantwortlichen oder eines Dritten
- Empfänger der personenbezogenen Daten

- die Absicht der Übermittlung an ein Drittland oder eine internationale Organisation
- Darüber hinaus ist der Betroffene zu informieren über:
- die voraussichtliche Dauer der Datennutzung
- die betroffenen Rechte auf Auskunft, Berichtigung, Löschung und eventuelle Einschränkungen dieser Rechte
- das Recht auf jederzeitigen Widerruf der Einwilligung
- das Beschwerderecht bei einer Aufsichtsbehörde
- die Bereitstellung der personenbezogenen Daten
- eine automatische Entscheidungsfindung

– **Erweiterung der Dokumentationspflichten:**

Eine zentrale Änderung durch die DSGVO ist die Einführung der „Rechenschaftspflicht“, welche gem. Art. 5 Abs. 2 DSGVO von den Verantwortlichen fordert, dass sie „die Einhaltung des Gesetzes nachweisen können“. Es reicht nicht mehr aus, sich nur an die Regelungen der Verordnung zu halten. Vielmehr müssen Unternehmen jederzeit die Rechtmäßigkeit der Datenverarbeitung nachweisen können.

Allein der **fehlende Nachweis** kann **hohe Bußgelder** zur Folge haben, auch wenn die Datenverarbeitung rechtmäßig erfolgte.

Im Zusammenhang mit der Rechenschaftspflicht steht das **Verzeichnis aller Datenverarbeitungsvorgänge**. [Art. 30 DSGVO](#) ordnet an, dass Verantwortliche und Auftragsdatenverarbeiter ein Verzeichnis über alle Verarbeitungstätigkeiten unter der Angabe der im Artikel genannten Punkte führen müssen.

Sofern eine Pflicht zur Führung eines solchen Verzeichnisses besteht, muss das Verzeichnis gem. Art. 30 DSGVO folgende Angaben enthalten:

- den Namen und die Kontaktdaten des Verantwortlichen und ggf. des gemeinsam mit ihm verantwortlichen Vertreters sowie eines etwaigen Datenschutzbeauftragten,
- die Zwecke der Verarbeitung,
- eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten,
- die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen,
- ggf. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation,
- wenn möglich die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien,

- wenn möglich eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen.

Auf Anfrage muss der Aufsichtsbehörde das Verarbeitungsverzeichnis vorgelegt werden. Die Pflicht zur Führung eines solchen Verzeichnisses **entfällt nur**, wenn:

- weniger als 250 Mitarbeiter beschäftigt werden **und**
- die Verarbeitung keine Risiken für die Rechte und Freiheiten der Betroffenen birgt **und**
- die Verarbeitung nur gelegentlich erfolgt **und**
- keine besonderen Datenkategorien gem. Art. 9 Abs. 1 DSGVO und Art. 10 DSGVO verarbeitet werden.

– **Einführung der Datenschutzfolgenabschätzung:**

Die DSGVO führt für die Verarbeitung von personenbezogenen Daten einen **risikobasierten Ansatz** ein. Ähnlich der bisherigen Vorabkontrolle sollen auf der Grundlage einer Risikoanalyse die Folgen der Verarbeitung abgeschätzt werden, um frühzeitig Schutzmaßnahmen ergreifen zu können. Es gilt: Je risikoreicher und schadensgeneigter eine Verarbeitung von Daten für Betroffene sein kann, umso höhere Anforderungen stellt die Verordnung an die Anwendung. Die DSGVO nennt in Art. 35 Abs. 3 bestimmte **Fallgruppen**, bei denen eine **Folgenabschätzung stets durchzuführen** ist.

Dazu gehören:

- das **Profiling**
- die **Verarbeitung besonders sensibler Daten** (Art. 9 Abs. 1 und Art. 10 DS-GVO)
- die **umfangreiche Videoüberwachung** öffentlich zugänglicher Bereiche

– **Erhöhung der Bußgelder**

Mit Inkrafttreten der DSGVO wird die Haftung erheblich verschärft. Bei Verstößen gegen die Grundprinzipien der Verordnung drohen Geldbußen von bis zu 20 Mio. EUR oder bis zu vier Prozent des weltweiten letztjährigen Jahresumsatzes. Für leichtere Verstöße gegen Pflichten aus der DSGVO ist ein Bußgeld von maximal zehn Mio. EUR oder von zwei Prozent des weltweiten letztjährigen Jahresumsatzes vorgesehen.

2. Weitere wesentliche Neuerungen der DSGVO sind:

– Räumlicher Anwendungsbereich (Marktortprinzip):

Das Europäische Datenschutzrecht gilt nach der Verordnung nicht nur für die in der EU niedergelassenen Unternehmen. Voraussetzung ist nach [Art. 3 Abs. 2 DSGVO](#) lediglich, dass sich ein Angebot an einen bestimmten nationalen **Markt in der EU** richtet oder dass die Datenverarbeitung der Beobachtung des Verhaltens von **Personen in der EU** dient. Der Anwendungsbereich erstreckt sich damit auch auf außereuropäische Unternehmen, die auf dem europäischen Markt tätig sind (Marktortprinzip).

– "Recht auf Vergessen werden":

Das Recht auf Löschung wird in [Art. 17 DSGVO](#) geregelt. Eine betroffene Person hat das Recht zur Löschung, wenn

- der Zweck der Verarbeitung entfallen ist,
- die betroffene Person der Verarbeitung widerspricht oder gegen die Verarbeitung Widerspruch einlegt,
- Verarbeitung der personenbezogenen Daten unrechtmäßig erfolgt,
- eine Pflicht des Verantwortlichen zur Löschung der Daten besteht oder
- der Betroffene als Kind seine Einwilligung zur Verarbeitung der Daten in den Fällen von Art. 8 DSGVO gegeben hat.

Das Recht zur Löschung besteht jedoch nicht in allen Fällen. Es gilt beispielsweise nicht, wenn die Verarbeitung **erforderlich** ist:

- zur Ausübung des Rechts auf freie Meinungsäußerung und Information,
- zur Erfüllung einer rechtlichen Verpflichtung oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in der Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde oder
- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

– Personenbezogene Daten von Kindern:

Zum ersten Mal ausdrücklich geregelt ist, dass eine Einwilligung in die Verarbeitung personenbezogener Daten erst im Alter von **16 Jahren** möglich ist ([Art. 8 DSGVO](#)). Zuvor bedarf es der elterlichen Einwilligung. Dabei ist wichtig, dass eine nachträgliche Genehmigung ausdrücklich ausgeschlossen ist. Die Mitgliedstaaten können auch ein niedrigeres Alter (Untergrenze 13 Jahre) vorsehen.

- **Prinzip des "One-Stop-Shop":**
Durch die DSGVO wird die Zuständigkeit der Aufsichtsbehörden vereinheitlicht. Mit dem Prinzip des „One-Stop-Shop“, zu Deutsch: das Prinzip der einheitlichen Anlaufstelle, wird festgehalten, dass künftig für grenzüberschreitende Datenvereinbarungen innerhalb der EU grundsätzlich die **Aufsichtsbehörde am Sitz der Hauptniederlassung** federführend zuständig sein wird.
- **Meldepflichten von Datenpannen:**
Die Verletzung des Schutzes personenbezogener Daten muss der Verantwortliche, bspw. das Unternehmen, ohne schuldhaftes Zögern und möglichst binnen 72 Stunden nachdem die Verletzung bekannt wurde, der zuständigen Aufsichtsbehörde melden, sofern nicht ein Risiko für die Rechte und Freiheiten natürlicher Personen ausgeschlossen ist ([Art. 33 DSGVO](#)).

VI. Wo gibt es weitere Informationen und praktische Hinweise?

Die Datenschutzkonferenz (ein Zusammenschluss verschiedener Datenschutzbehörden des Bundes und der Länder) hat etliche **Kurzpapiere zu verschiedenen Themen** und Fragen der DSGVO veröffentlicht. Dort sind auch **praktische Empfehlungen** enthalten. Einige der Papiere finden Sie auf dieser Seite oben rechts, eine Übersicht aller bisher erschienenen Papier [hier](#).

Hinsichtlich eines Löschkonzepts hat das [Deutsche Institut für Normung e.V.](#) die [DIN 66398](#) herausgegeben, die als Leitlinie und Orientierung dienen kann.

Wir danken der IHK Koblenz für die Erarbeitung und Bereitstellung der Informationen.

Dieses Merkblatt soll - als Service Ihrer IHK - nur erste Hinweise geben und erhebt daher keinen Anspruch auf Vollständigkeit. Obwohl es mit größtmöglicher Sorgfalt erstellt wurde, kann eine Haftung für die inhaltliche Richtigkeit nicht übernommen werden.